

TITLE: Covert Authentication Method and Apparatus

5 Related Applications

No other applications relate

10 Field of the invention

The invention relates to authentication systems and to a field known as “security printing”.

15 Background of the invention

There is a need to mark certain items to avoid counterfeiting. Marked items can be monetary tools such as banknotes, stamps, checks etc or government documents such as passports, visas etc. They can also be high value commercial items. Sometimes the authenticated items are pharmaceutical, to protect not only the monetary value but also the safety of the users. Most systems need to be verified by machine reading, sometimes through a wrapper or enclosure. One class of solutions uses a small amount of an additive, known as a taggant. The taggant can be detected with a specialized detector but is not visible under normal conditions. The advantage of a taggant is, besides being covert, is that it can be made machine-readable at high speeds. At very small doses it can be very difficult to find and identify, unless the specialized detector is

used. The disadvantage of tagging is that it can carry a limited number of combinations, particularly if it has to be machine-readable. This does not allow giving each item a unique identification code or secure serial number (the visible serial number or barcode printed on most items can be easily counterfeited). To make it harder to counterfeit some

5 systems use a random distribution of fibers or patterns, but because they rely on simple optical scanning for reading, a simple photocopy of the image will also read as genuine in most cases.

Summary of the invention

The invention relies on the random patterns created when a small quantity of a tagging powder, or taggant, is mixed with a material used in an item. The taggant can be dispersed in paper, printing inks, varnishes, paints, adhesives, plastics and even molten metals (as long as a taggant compatible with high temperatures is selected). The taggant is invisible to the eye (even under magnification) but can be made highly visible by creating the right conditions such as illumination with UV light, heating, chemical activation etc. When viewed under those conditions, a unique taggant image is captured from each item and stored in a database. When an item has to be authenticated, the taggant image is captured again and compared to the images stored in the database. Only items that match the database are recognized as genuine items. The degree of matching required does not have to be 100% as some of the taggant may be missing or masked. A preset threshold of matching can be used. Because of the uniqueness of each image, even less than full matching identifies the item with a high level of reliability.

Brief description of the drawings

Fig 1-a to Fig 1-f show the steps required in creating and identifying a tagged item according to the invention.

Fig 2 shows the apparatus used to see and process the taggant image.

Fig 3 shows schematically the method used to compare the taggant image to the images stored in the database.

Description of the preferred embodiment

While the taggant can be detected by any physical or chemical property, such as light, magnetism, reactivity etc the preferred embodiment uses an optical method of detection.

- 5 The main advantage of the optical detection method is that the unique image of the taggant distribution can be captured by a simple and inexpensive CCD or CMOS camera. In order to make the taggant invisible (unless the correct detector is used), a very fine powder is used in a very low concentration (down to a few parts per million). Such a powder, particularly if it has a color matching the background color, is very
- 10 difficult to detect even by forensic methods.

- In order to detect and capture the image of the powder it has to be made highly visible. This is achieved by a special detector. Typically, the detector will contain a shroud blocking ambient light or other electromagnetic radiation. Within the detector, a special
- 15 environment is set up to make the powder highly visible relative to the background. By way of example, the taggant can be a fluorescent powder and the special environment making it highly visible is Ultra Violet (UV) light. Such fluorescent powders are widely used in fluorescent inks and markers, are readily available, stable and inexpensive. Particle size should be in the 5-50um range. If a higher level of security is required, the
- 20 taggant can be a completely optically and chemically inert powder with thermal properties different from those of the background.

- When exposed to a pulse of intense light (at almost any part of the spectrum) and viewed with a camera sensitive to the 5um-10um range of the IR spectrum, the taggant
- 25 particles will appear brighter or darker than the background, depending on their thermal properties. The light pulse should have duration from 0.1mS to 50mS, preferable 1-5mS,

and the viewing should be within a few mS of the pulse. The camera used for viewing can be of the microbolometer type. The light source can be a standard camera electronic flash unit. By way of example, the taggant can be aluminum or stainless steel powder, glass or polystyrene microspheres, or alumina (Al_2O_3) powder. Materials heating up less than the background will show up as dark dots, materials heating up more will show up as light dots. Particle size should be in the 20-50um range. A very similar system used to detect small defects in copper traces is disclosed in US patent 6,340,817 (having the same inventor and assignee as the current application).

Further details on the construction of the detector are given in Fig 2. An item 1, such as a printed label, is tagged by mixing taggant particles 3 in the substrate material or ink in order to permanently anchor the taggant to the substrate. Concentration can be as low as a few parts per million by weight. The detector 4 comprises of a camera 6, focused on the surface of item 1 using lens 5. An optical filter 13 blocks the excitation light, generated by pulsed source 8, from the camera. A shroud 5 blocks ambient light. The output of the camera (typically NTSC video) is converted to a binary image using comparator 9. The threshold of comparator 5 is automatically set by processing unit 11 via feedback 10 to generate a fixed number of detected taggant particles (more details on this are given later). The output is fed as serial data stream 12, giving the coordinates of the taggant particles. Obviously, the data can be encrypted, if desired, for even greater security. For UV fluorescence, light source 8 is a high power UV LEDs (Nichia part # NCCU001E, 10 LEDs used in parallel) and Filter 13 is an interference filter with a bandwidth and center wavelength matched to the fluorescent powder selected. Filters 14 block any light above a wavelength of 0.4um. For best results, yellow or red fluorescent powders are used, as many substrates have blue fluorescence used as a whitener (the colors mentioned refer to the emitted light, not to the color of the powder in the unexcited

state, which is typically white). For the thermal taggants the light sources 8 are a camera flash unit and filter 13 is a long pass filter blocking any light below 3 μ m. Filter 14 is a short pass filter blocking any light above 2 μ m (in order to avoid blinding of the camera by the flash units). The camera is of the microbolometer type. By way of example, good results were obtained with an AGEMA microbolometer camera model 570 and a close-up lens. A second light source, 8', may be required if the registration mark (item 2 in Fig 1) is not clearly visible under the illumination of filtered light source 8.

The steps needed to practice the invention are shown in Fig 1. Fig1-a shows an item 1, by the way of example a document or a security label. A reference mark 2 is selected to register the taggant image. The edges of the item can also be used as a reference, when nothing is printed on it. The reference mark can be a line, a company logo, a frame etc. In the normal mode the taggant is not visible. While item 1 was made (or printed) taggant 3 was added and the taggant distribution is shown in Fig1-b. Fig 1-b visualized the distribution, which is not normally visible. The taggant 3 can also be added selectively, for example by mixing it only with a particular ink or varnish, as shown in Fig 1-c. When the detector 4 is placed over item 1 it does not need to be aligned with it, as shown in Fig 1-d., as long as it covers the area of interest. The camera in the detector sees the taggant 3 in the area of interest, frame 2, as shown in Fig 1-e. The image appears rotated, as the detector was not aligned with item 1. The processor 11 in Fig 2 includes software to recognize the reference mark 2 and rotate the image to align it with the horizontal and vertical axis (or any selected reference axis). The subsystem comprising the camera, lens, electronics and image registration and rotation software is available as a standard package from suppliers of machine vision systems. By the way of example, a compact package in the InSight product line made by Cognex (Natick, Ma.). As explained earlier, the processor output can set the threshold of the comparator

9 in Fig 2 to always have the same number of taggant particles detected, in order to simplify the data base. Since the taggant particles have a distribution of sizes, changing the threshold changes the number of particles whose signal will exceed the threshold. A fixed threshold, variable particle count can also be used. The processed image appears
5 in Fig 1-f.

By way of example, the system was set to detect six particles of taggant 3 within the reference frame 2. The coordinates of each particle are sent out as x-y pairs, X1Y1; X2Y2;.....X6Y6. The best number of particles depends on the size of the database, but
10 a preferred range is from 2 to 100 particles. By way of example, if the camera has a resolution of 600x400 pixels and this is divided into a coarser grid of 256x256, the area of the reference frame 2 is about 100x100 pixels. With 6 particles this allows almost $(100 \times 100)^6 = 10^{24}$ different images. Even accepting partial matches of 5 out of the 6 particles, this allows billions of unique images. At the same time the image storage
15 requirements and data transmission requirements (from the detector to the data base) are minimal, as each one of the six particles is defined by two bytes (XnYn) for a total of only 12 bytes of data – only 12Gbytes for a billion images.

The authentication process is shown schematically in Fig 3. When each item is recorded
20 into the database, it is read by the detector shown in Fig 2 and the output data 12, which is 12 bytes in this example, is stored in the database 23 in Fig 3. Since the images are random, they can be stored sequentially in the database; that is, there is no preferred order. For large databases, special algorithms can be used to “classify” the images for faster retrieval. When an item has to be authenticated (such as a passport at the border
25 or a label on a product), the item is read by the detector and the processed taggant image (Fig 1-f) is sent as data 12 from the detector to the verification unit shown in Fig 3.

There the data 12 is stored in a register 18 and is compared to all the images in the database 23 until a match is found. The images are read out from database 23 into a register 17, and comparators 19 check for matches. In this example there are six comparators for the six taggant particles. The output of the comparators (COM1, COM2.....COM6) are fed to a logic circuit 20 which is programmed with the number of matches which have to be reached before a "Pass" signal is generated. For six particles, a good threshold is four or five matches. Requiring six matches will cause problems in cases that a taggant particle was obstructed, missing or not detected. The "Pass" signal can be sent back from the verification unit to the detector. The data links can be over phone lines, wireless, Internet or any other means. The required data rate is very low: to verify 100 items per second the data rate is only $100 \times 12 \text{ bytes} = 1200$ Bytes/sec in this example. For large databases and very rapid identification, at least part of database 23 has to be in Random Access Memory (RAM) as images have to be compared quickly. For increased throughput, the database can have multiple parallel ports 24, each connected to a different section, and all sections checked in parallel. This requires only the duplication of items 17, 18, 19, 20, which are low cost items.

In some cases the dependence on a remote database is not desired and the system can be used in a "stand alone" mode. In this mode a code is printed on each item at the time it is read by the detector for the first time. This code is derived from the taggant location and can be as simple as the taggant coordinates $X_n Y_n$ or an encrypted version of it. Each time the item is read for authentication, a code is generated using the same rules and the code is compared to the code printed on the item. If they match, the item is authentic. Even if the code is copied onto a counterfeit item, it will not match the unique taggant distribution. If the code is machine readable, such as a barcode, the complete authentication process can be automated. Any combination of this "stand alone" mode

and verification against a database can be used. For example, if the database is not functional, the "stand alone" mode can be used. The advantage of the database is that other information can be attached to each item in the database.

5 Clearly the high level of security this invention provides does not depend on the taggant used, only on the fact that it is nearly impossible to duplicate the random patterns it generates. Unlike other tagging systems, the security is not compromised even if the taggant is known and available to counterfeiters. What cannot be duplicated is the random distribution. The type of taggant used and method of detecting it is not
10 important. The main reason for making the taggant invisible is in order not to alert anyone that an authentication system is used; when this is not an issue, the system can be simplified by using a visible taggant or applying a random pattern via spraying of paint etc. However, it is always more desirable to mix the taggant into one of the materials forming the item and making the taggant invisible to the human eye.

15

There have thus been outlined the important features of the invention in order that it may be better understood, and in order that the present contribution to the art may be better appreciated. Those skilled in the art will appreciate that the conception on which this disclosure is based may readily be utilized as a basis for the design of other
20 compositions, elements and methods for carrying out the several purposes of the invention. It is most important, therefore, that this disclosure be regarded as including such equivalent compositions, elements and methods as do not depart from the spirit and scope of the invention.